NIAC Working Group on Prioritization of Cyber Vulnerabilities

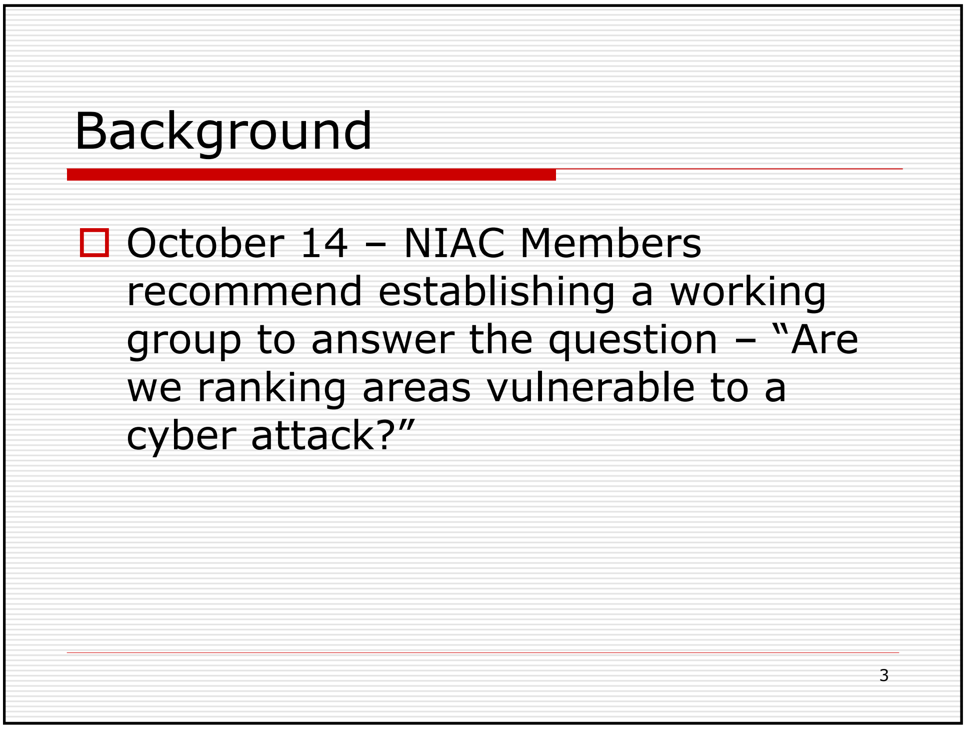
Working Group Update

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday – July 13, 2004

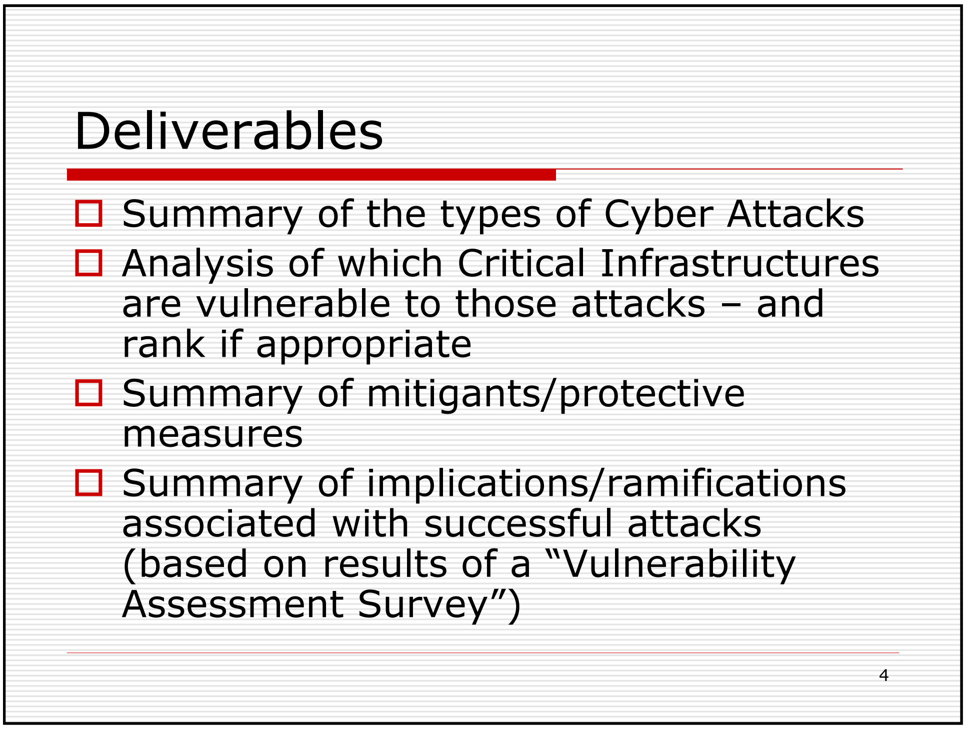
Presentation Outline

- □ Background
- □ Deliverables
- □ Survey Content
- □ Report on Actions to Date
- □ Critical Infrastructures Surveyed
- □ Preliminary Observations
- □ Next Steps
- □ Appendix



Background

- □ October 14 – NIAC Members recommend establishing a working group to answer the question – “Are we ranking areas vulnerable to a cyber attack?”



Deliverables

- □ Summary of the types of Cyber Attacks
- □ Analysis of which Critical Infrastructures are vulnerable to those attacks – and rank if appropriate
- □ Summary of mitigants/protective measures
- □ Summary of implications/ramifications associated with successful attacks (based on results of a “Vulnerability Assessment Survey”)

Survey Content

- □ Identification of key information systems and what they accomplish
- □ Economic metrics of these systems
- □ Implications to National Security/Emergency Preparedness
- □ Dependency on any other network based critical infrastructure
- □ Dependency of a critical infrastructure on this service
- □ Implications of various types of cyber attacks on these key systems

Report on Actions Taken to Date

□ Survey Finalized	April 28
□ Survey Distribution	April 30
□ Return Date for Surveys	May 26
□ Follow Up	June
□ Compilation and analysis	July 10

Critical Infrastructures Surveyed and

✓ *Responses Received to date*

☑ Telecommunications
☐ Information Technology
☑ Transportation
☑ Postal and Parcel Shipping
☑ Banking and Finance
☑ Public Health and Health Care
☐ Agriculture and Food
☑ Water
☑ Energy
☐ Defense Industry Base
☐ Chemical
☐ Government Emergency Services

Preliminary Observations

Weighted Rankings of Dependencies

1. Telecom
2. Energy
3. Banking
4. Postal
5. Transportation
6. Water
7. Food
8. EMS
9. Chemical
10. Public Health
11. IT

Other Preliminary Observations

- □ Respondents very concerned about confidentiality of data.
- □ Answers are dependent upon the nature and duration of disaster.
- □ Sound business continuity practices provide some protection:
  - ■ Ability to revert to back up systems, and further ability to revert to manual systems, though less efficient, can minimize impact in some sectors.
  - ■ Inefficiency of manual procedures would result in increased costs or lost revenue for some sectors.
  - ■ Redundancy expense is often already realized as part of existing business continuity programs.
  - ■ System restoration would happen more often than system replacement.
  - ■ Costs to reconstruct data, or to run in a manual mode, would be great.
  - ■ Diversity of vendors within core systems provides some additional protection.

Next Steps

- □ Addition of any late surveys
- □ Finalize analysis
- □ Submit report to NIAC for review

Appendix

- □ Working Group Participants

Study Group Participants

- Susan Vismor, Mellon Financial Corp., Study Group Chair
- Teresa C. Lindsey, BITS
- Peter Allor – Internet Security Systems
- Bruce Larsen – American Water
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Dan Bart, TIA
- David Thompson, TIA
- Lou Leffler, North American Electric Power
- Tim Zoph, Northwestern Memorial Hospital
- Scott Borg, Institute for Security Technology Studies, Dartmouth College
- Nancy Wong, DHS
- Gail Kaufman, DHS
- David Sanders, DHS, National Cyber Security Division
    - □ Tran Trang, NCSD

Cyber-Attack Models

Types of Cyber Incidents (CERT)

- Probe
- Scan
- Account Compromise
- Root Compromise
- Packet Sniffer
- Denial of Service
- Exploitation of Code
- Internet Infrastructure Attacks

Information Security Model

- Confidentiality
- Availability
- Integrity
- Authentication
- Non-repudiation

Business Categories (Borg Model)

- Interruption of data in order to interrupt business operations
- Corruption of data in order to cause it to operate defectively
- Obfuscation of data, causing people to be in the wrong business
- Publication of confidential data, undermining the ability to engage in any business

Technical Exploit → *Compromises Security* → *Business Impact*

Survey Content

- □ Identification of key information systems and what they accomplish
- □ Economic metrics of these systems
- □ Implications to National Security/Emergency Preparedness
- □ Dependency on any other network based critical infrastructure
- □ Dependency of a critical infrastructure on this service

Survey Content

- Evaluate the possible consequences of “types” of cyber attacks on each of the identified key systems:
  - Interruption of business operations
  - Business operates in a defective way
  - Distrust of the system
  - Undermine the ability to engage in that business

Survey Content

- Identifying what alternatives might be utilized in the event of a sustained attack on each of these systems